

CLAIMS

What is claimed is:

1. A method for monitoring a server application in a computer network, the method comprising:
  - 5 (a) monitoring communication data between a server application and a client;
  - (b) applying at least one detector to the communication data to identify at least one predetermined activity; and
  - 10 (c) generating a threat score associated with the predetermined activity by comparing the identified predetermined activity with a security threshold criteria.
2. The method of claim 1, comprising selectively generating an alert based upon the threat score associated with the at least one detector.
- 15 3. The method of claim 1, wherein steps (a) – (c) are performed transparent to the communication of data between the server application and the client.
- 20 4. The method of claim 1, wherein the communication data is communicated over a network selected from the group consisting of a global communication network, a wide area network, a local area network, and a wireless network.
- 25 5. The method of claim 1, wherein the communication data comprises an application protocol selected from the group consisting of hypertext transfer protocols, simple object access protocols, web distributed authoring and versioning protocols, simple mail transfer protocols, wireless application protocols, file transfer protocols, Internet message access  
30 protocols, post office protocols, web services protocols, simple mail transfer protocols, structured hypertext transfer protocols, and web-mail protocols.

6. The method of claim 1, wherein the communication data can comprise HTTP requests from the client and HTTP responses from the server application.

5 7. The method of claim 1, wherein the server application is implemented by a web server.

8. The method of claim 1, wherein the client is implemented by a web-enabled device including a unique Internet protocol (IP) address.

10

9. The method of claim 1, wherein the communication data comprises only transmission control protocol packets.

10. The method of claim 1, comprising associating the at least one predetermined activity with a unique communication session between the server application and the client.

15

11. The method of claim 10, wherein the unique communication session is a login session wherein the server application has been provided at least a user name and password from the client.

20

12. The method of claim 1, wherein step (b) comprises associating the threat score with an object selected from the group consisting of the client, a computer, an IP address, a web user and/or session, an application, or a server client.

25

13. The method of claim 1, wherein the at least one detector generates a threat score when the at least one predetermined activity deviates a predetermined amount from the security threshold criteria.

30

14. The method of claim 13, wherein the security threshold criteria is an expected activity for the client.

5 15. The method of claim 1, wherein the at least one detector identifies when the communication data from the client is associated with an predetermined user.

10 16. The method of claim 1, wherein the predetermined activity is login activity.

17. The method of claim 1, wherein the predetermined activity is form manipulation.

15 18. The method of claim 1, wherein the predetermined activity is session cookie manipulation.

19. The method of claim 1, wherein the predetermined activity is protocol activity.

20 20. The method of claim 1, wherein the predetermined activity is URL encoding.

25 21. The method of claim 1, wherein the at least one detector is a plurality of detectors.

22. The method of claim 1, comprising adding the threat scores accumulated by the at least one detector to generate a total threat score.

30 23. The method of claim 1, comprising displaying the alert to an operator.

24. The method of claim 1, comprising displaying the threat score associated with the at least one detector.

5 25. The method of claim 1, comprising providing a user interface for enabling an operator to configure the security threshold criteria.

26. A system for monitoring a server application in a computer network, the system comprising:

- 10 (a) a network interface operable to monitor communication data between a server application and a client; and
- (b) a detector operable to identify at least one predetermined activity in the monitored communication data, and generate a threat score associated with the predetermined activity by comparing the identified predetermined activity with a security threshold
- 15 criteria.

27. The system of claim 26, a user interface operable to selectively generate an alert based upon the threat score associated with the detector.

20 28. The system of claim 26, wherein the communication data is communicated over a network selected from the group consisting of a global communication network, a wide area network, a local area network, and a wireless network.

25 29. The system of claim 26, wherein the communication data comprises an application protocol selected from the group consisting of hypertext transfer protocols, simple object access protocols, web distributed authoring and versioning protocols, simple mail transfer protocols, wireless application protocols, file transfer protocols, Internet message access

30 protocols, post office protocols, web services protocols, simple mail transfer protocols, structured hypertext transfer protocols, and web-mail protocols.

30. The system of claim 26, wherein the communication data can comprise HTTP requests from the client and HTTP responses from the server application.

5           31. The system of claim 26, wherein the server application is implemented by a web server.

32. The system of claim 26, wherein the client is implemented by a web-enabled device including a unique Internet protocol (IP) address.

10

33. The system of claim 26, wherein the communication data comprises only transmission control protocol packets.

34. The system of claim 26, comprising a session detector operable to associate the at least one predetermined activity with a unique communication session between the server application and the client.

15

35. The system of claim 34, wherein the unique communication session is a login session wherein the server application has been provided at least a user name and password from the client.

20

36. The system of claim 26, wherein the detector can associate the threat score with an object selected from the group consisting of the client, computer, IP address, web user and/or session, application, or server client.

25

37. The system of claim 26, wherein the detector is operable to generate a threat score when the at least one predetermined activity deviates a predetermined amount from the security threshold criteria.

30

38. The system of claim 37, wherein the security threshold criteria is an expected activity for the client.

39. The system of claim 26, wherein the detector is operable to identify when the communication data from the client is associated with an predetermined user.

5           40. The system of claim 26, wherein the predetermined activity is login activity.

          41. The system of claim 26, wherein the predetermined activity is form manipulation.

10

          42. The system of claim 26, wherein the predetermined activity is session cookie manipulation.

          43. The system of claim 26, wherein the predetermined activity is protocol activity.

15

          44. The system of claim 26, wherein the predetermined activity is URL encoding.

20           45. The system of claim 26, wherein the detector is a plurality of detectors.

          46. The system of claim 26, comprising a display for displaying the alert to an operator.

25

          47. The system of claim 26, comprising a display for displaying the threat score associated with the at least one detector.

          48. The system of claim 26, comprising a user interface for enabling an operator to configure the security threshold criteria.

30

49. A computer program product comprising computer-executable instructions embodied in a computer-readable medium for performing steps comprising:

5

(a) monitoring communication data between a server application and a client;

(b) applying at least one detector to the communication data to identify at least one predetermined activity; and

10

(c) generating a threat score associated with the predetermined activity by comparing the identified predetermined activity with a security threshold criteria.

15

50. The computer program product of claim 49, comprising selectively generating an alert based upon the threat score associated with the at least one detector.

51. The computer program product of claim 49, wherein steps (a) – (c) are performed transparent to the communication of data between the server application and the client.

20

52. The computer program product of claim 49, wherein the communication data is communicated over a network selected from the group consisting of a global communication network, a wide area network, a local area network, and a wireless network.

25

53. The computer program product of claim 49, wherein the communication data comprises an application protocol selected from the group consisting of hypertext transfer protocols, simple object access protocols, web distributed authoring and versioning protocols, simple mail transfer protocols, wireless application protocols, file transfer protocols, Internet message access protocols, post office protocols, web services protocols, simple mail transfer protocols, structured hypertext transfer protocols, and web-mail protocols.

30

54. The computer program product of claim 49, wherein the communication data can comprise HTTP requests from the client and HTTP responses from the server application.

5 55. The computer program product of claim 49, wherein the server application is implemented by a web server.

10 56. The computer program product of claim 49, wherein the client is implemented by a web-enabled device including a unique Internet protocol (IP) address.

57. The computer program product of claim 49, wherein the communication data comprises only transmission control protocol packets.

15 58. The computer program product of claim 49, comprising associating the at least one predetermined activity with a unique communication session between the server application and the client.

20 59. The computer program product of claim 58, wherein the unique communication session is a login session wherein the server application has been provided at least a user name and password from the client.

25 60. The computer program product of claim 49, wherein step (b) comprises associating the threat score with an object selected from the group consisting of the client, computer, IP address, web user and/or session, application, or server client.

30 61. The computer program product of claim 49, wherein the at least one detector generates a threat score when the at least one predetermined activity deviates a predetermined amount from the security threshold criteria.

62. The computer program product of claim 61, wherein the security threshold criteria is an expected activity for the client.

5 63. The computer program product of claim 49, wherein the at least one detector identifies when the communication data from the client is associated with an predetermined user.

10 64. The computer program product of claim 49, wherein the predetermined activity is login activity.

65. The computer program product of claim 49, wherein the predetermined activity is form manipulation.

15 66. The computer program product of claim 49, wherein the predetermined activity is session cookie manipulation.

67. The computer program product of claim 49, wherein the predetermined activity is protocol activity.

20 68. The computer program product of claim 49, wherein the predetermined activity is URL encoding.

25 69. The computer program product of claim 49, wherein the at least one detector is a plurality of detectors.

70. The computer program product of claim 49, comprising adding the threat scores accumulated by the at least one detector to generate a total threat score.

30 71. The computer program product of claim 49, comprising displaying the alert to an operator.

72. The computer program product of claim 49, comprising displaying the threat score associated with the at least one detector.

5 73. The computer program product of claim 49, comprising providing a user interface for enabling an operator to configure the security threshold criteria.

74. A method for monitoring a server application in a computer network, the method comprising:

- 10 (a) monitoring communication data between a server application and a client;
- (b) applying a plurality of detectors to the communication data, wherein each detector detects different predetermined activity associated with the data communication between the server application and the client;
- 15 (c) generating an individual threat score for each detector based upon detection of the predetermined activity by each detector; and
- (d) generating an overall threat score for the client by combining the individual threat scores.
- 20

75. The method of claim 74, comprising selectively generating an alert based upon the overall threat score.

25 76. The method of claim 74, wherein steps (a) – (d) are performed transparent to the communication of data between the server application and the client.

30 77. The method of claim 74, wherein the communication data is communicated over a network selected from the group consisting of a global

communication network, a wide area network, a local area network, and a wireless network.

5           78.    The method of claim 74, wherein the communication data  
comprises an application protocol selected from the group consisting of  
hypertext transfer protocols, simple object access protocols, web distributed  
authoring and versioning protocols, simple mail transfer protocols, wireless  
application protocols, file transfer protocols, Internet message access  
10       protocols, post office protocols, web services protocols, simple mail transfer  
protocols, structured hypertext transfer protocols, and web-mail protocols.

          79.    The method of claim 74, wherein the communication data can  
comprise HTTP requests from the client and HTTP responses from the server  
application.

15

          80.    The method of claim 74, wherein the server application is  
implemented by a web server.

          81.    The method of claim 74, wherein the client is implemented by a  
20       web-enabled device including a unique Internet protocol (IP) address.

          82.    The method of claim 74, wherein the communication data  
comprises only transmission control protocol packets.

25           83.    The method of claim 74, comprising associating the  
predetermined activity with a unique communication session between the  
server application and the client.

          84.    The method of claim 83, wherein the unique communication  
30       session is a login session wherein the server application has been provided at  
least a user name and password from the client.

85. The method of claim 74, wherein step (d) comprises associating the overall threat score with the client.

5 86. The method of claim 74, wherein at least one of the detectors generates a threat score when the at least one predetermined activity deviates a predetermined amount from the security threshold criteria.

10 87. The method of claim 86, wherein the security threshold criteria is an expected activity for the client.

88. The method of claim 74, wherein at least one of the detectors identifies when the data communication from the client is associated with an predetermined user.

15 89. The method of claim 74, wherein one of the predetermined activity is login activity.

20 90. The method of claim 74, wherein one of the predetermined activity is form manipulation.

91. The method of claim 74, wherein one of the predetermined activity is session cookie manipulation.

25 92. The method of claim 74, wherein one of the predetermined activity is protocol activity.

93. The method of claim 74, wherein one of the predetermined activity is URL encoding.

30 94. The method of claim 74, comprising adding the threat scores accumulated by the detectors to generate a total threat score.

95. The method of claim 74, comprising selectively generating an alert based upon the overall threat score.

5 96. The method of claim 95, comprising displaying the alert to an operator.

97. The method of claim 74, comprising displaying the individual threat scores associated with the detectors.

10 98. The method of claim 74, comprising providing a user interface for enabling an operator to configure the detectors.

99. A system for monitoring a server application in a computer network, the system comprising:

- 15 (a) a network interface operable to monitor communication data between a server application and a client; and
- (b) a plurality of detectors operable to detect different predetermined activity associated with the monitored communication data, generate an individual threat score for each detector based upon
- 20 detection of the predetermined activity by each detector, and generate an overall threat score for the client by combining the individual threat scores.

25 100. The system of claim 99, comprising a user interface for selectively generating an alert based upon the overall threat score.

30 101. The system of claim 99, wherein the communication data is communicated over a network selected from the group consisting of a global communication network, a wide area network, a local area network, and a wireless network.

5           102. The system of claim 99, wherein the communication data comprises an application protocol selected from the group consisting of hypertext transfer protocols, simple object access protocols, web distributed authoring and versioning protocols, simple mail transfer protocols, wireless application protocols, file transfer protocols, Internet message access protocols, post office protocols, web services protocols, simple mail transfer protocols, structured hypertext transfer protocols, and web-mail protocols.

10           103. The system of claim 99, wherein the communication data can comprise HTTP requests from the client and HTTP responses from the server application.

15           104. The system of claim 99, wherein the server application is implemented by a web server.

          105. The system of claim 99, wherein the client is implemented by a web-enabled device including a unique Internet protocol (IP) address.

20           106. The system of claim 99, wherein the communication data comprises only transmission control protocol packets.

          107. The system of claim 99, comprising a session detector operable to associate the predetermined activity with a unique communication session between the server application and the client.

25           108. The system of claim 107, wherein the unique communication session is a login session wherein the server application has been provided at least a user name and password from the client.

109. The system of claim 99, wherein at least one of the detectors generates a threat score when the at least one predetermined activity deviates a predetermined amount from the security threshold criteria.

5           110. The system of claim 109, wherein the security threshold criteria is an expected activity for the client.

10           111. The system of claim 99, wherein at least one of the detectors identifies when the communication data from the client is associated with an predetermined user.

112. The system of claim 99, wherein one of the predetermined activity is login activity.

15           113. The system of claim 99, wherein one of the predetermined activity is form manipulation.

20           114. The system of claim 99, wherein one of the predetermined activity is session cookie manipulation.

115. The system of claim 99, wherein one of the predetermined activity is protocol activity.

25           116. The system of claim 99, wherein one of the predetermined activity is URL encoding.

117. The system of claim 99, comprising a display displaying the individual threat scores associated with the detectors.

30           118. The system of claim 99, comprising a user interface for enabling an operator to configure the detectors.

119. A computer program product comprising computer-executable instructions embodied in a computer-readable medium for performing steps comprising:

- 5 (a) monitoring communication data between a server application and a client;
- (b) applying a plurality of detectors to the communication data, wherein each detector detects different predetermined activity associated with the data communication between the server application and the client;
- 10 (c) generating an individual threat score for each detector based upon detection of the predetermined activity by each detector; and
- (d) generating an overall threat score for the client by combining the individual threat scores.

15

120. The computer program product of claim 119, comprising selectively generating an alert based upon the overall threat score.

20 121. The computer program product of claim 119, wherein steps (a) – (d) are performed transparent to the communication of data between the server application and the client.

25 122. The computer program product of claim 119, wherein the communication data is communicated over a network selected from the group consisting of a global communication network, a wide area network, a local area network, and a wireless network.

30 123. The computer program product of claim 119, wherein the communication data comprises an application protocol selected from the group consisting of hypertext transfer protocols, simple object access protocols, web distributed authoring and versioning protocols, simple mail transfer protocols,

wireless application protocols, file transfer protocols, Internet message access protocols, post office protocols, web services protocols, simple mail transfer protocols, structured hypertext transfer protocols, and web-mail protocols.

5           124. The computer program product of claim 119, wherein the communication data can comprise HTTP requests from the client and HTTP responses from the server application.

10           125. The computer program product of claim 119, wherein the server application is implemented by a web server.

15           126. The computer program product of claim 119, wherein the client is implemented by a web-enabled device including a unique Internet protocol (IP) address.

127. The computer program product of claim 119, wherein the communication data comprises only transmission control protocol packets.

20           128. The computer program product of claim 119, comprising associating the predetermined activity with a unique communication session between the server application and the client.

25           129. The computer program product of claim 119, wherein the unique communication session is a login session wherein the server application has been provided at least a user name and password from the client.

130. The computer program product of claim 119, wherein step (d) comprises associating the overall threat score with the client.

131. The computer program product of claim 119, wherein at least one of the detectors generates a threat score when the at least one predetermined activity deviates a predetermined amount from the security threshold criteria.

5           132. The computer program product of claim 131, wherein the security threshold criteria is an expected activity for the client.

10           133. The computer program product of claim 119, wherein at least one of the detectors identifies when the data communication from the client is associated with an predetermined user.

134. The computer program product of claim 119, wherein one of the predetermined activity is login activity.

15           135. The computer program product of claim 119, wherein one of the predetermined activity is form manipulation.

20           136. The computer program product of claim 119, wherein one of the predetermined activity is session cookie manipulation.

137. The computer program product of claim 119, wherein one of the predetermined activity is protocol activity.

25           138. The computer program product of claim 119, wherein one of the predetermined activity is URL encoding.

139. The computer program product of claim 119, comprising adding the threat scores accumulated by the detectors to generate a total threat score.

30           140. The computer program product of claim 119, comprising selectively generating an alert based upon the overall threat score.

141. The computer program product of claim 140, comprising displaying the alert to an operator.

5 142. The computer program product of claim 119, comprising displaying the individual threat scores associated with the detectors.

143. The computer program product of claim 119, comprising providing a user interface for enabling an operator to configure the detectors.